



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11)Publication number: 07249264

(43)Date of publication of application: 26.09.1995

(51)Int.Cl.

G11B 20/10
G06F 12/14

(21)Application number: 06065426

(71)Applicant:

INTEC:KK
BROTHER IND LTD
KAWASAKI TETSUO
HOSHIBA SHINJI
TANIGUCHI TOSHINORI

(22)Date of filing: 10.03.1994

(72)Inventor:

(54) RECORDING SYSTEM AND RECORDING/REPRODUCING SYSTEM FOR CD-ROM, AND CD-ROM DISK

(57)Abstract:

PURPOSE: Tounnecessary control of key information for deciphering ciphered data recorded in a CD-ROM disk.

CONSTITUTION: When desired information is ciphered and recorded in the CD-ROM disk 1, key information required for decoding this ciphered information is recorded in a proper region 3 in the CD-ROM disk 1 with the ciphering information. When recorded contents of the CD-ROM disk 1 in which ciphering information is recorded by this recording system are reproduced, a desired key information is read out from the same CD-ROM disk 1 with ciphering information, and the ciphered information can be deciphered by only this read-out information.

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開平7-249264

(43)公開日 平成7年(1995)9月26日

(51)Int.C1.⁶ 識別記号 庁内整理番号 F I 技術表示箇所
G 1 1 B 20/10 H 7736-5 D
G 0 6 F 12/14 3 2 0 B

審査請求 未請求 請求項の数3 FD (全9頁)

(21)出願番号	特願平6-65426	(71)出願人 391021710 株式会社インテック 富山県富山市牛島新町5番5号
(22)出願日	平成6年(1994)3月10日	(71)出願人 000005267 プラザー工業株式会社 愛知県名古屋市瑞穂区苗代町15番1号
		(72)発明者 河崎 哲男 富山県富山市下新町3番23号 株式会社インテック内
		(72)発明者 干場 進二 富山県富山市下新町3番23号 株式会社インテック内
		(74)代理人 弁理士 高野 昌俊

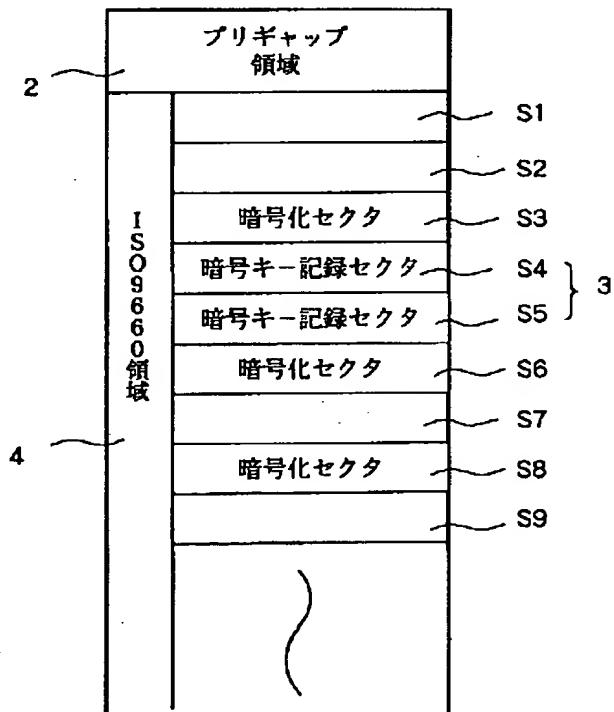
最終頁に続く

(54)【発明の名称】CD-ROMの記録方式、記録・再生方式及びCD-ROMディスク

(57)【要約】

【目的】 CD-ROMディスクに記録された暗号化データの解読のためのキー情報の管理を不要にすること。

【構成】 所要の情報を暗号化してCD-ROMディスク(1)に記録するさい、この暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該CD-ROMディスク(1)内の適宜の領域(3)に記録する。このような記録方式で暗号化情報が記録されているCD-ROMディスクの記録内容を再生する場合には、暗号化情報と共に所要のキー情報が同一のCD-ROMディスクから読み出され、これらの読み出し情報のみによって暗号化情報を復号化することができる。



【特許請求の範囲】

【請求項1】 所要の情報を暗号化してCD-ROMディスクに記録するためのCD-ROMの記録方式において、CD-ROMディスクに記録すべき暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該CD-ROMディスク内に記録しておくことを特徴とするCD-ROMの記録方式。

【請求項2】 所要の情報を暗号化してCD-ROMディスクに記録しこの記録された暗号化情報をCD-ROMディスクから読み出して復号化するためのCD-ROMの記録・再生方式において、CD-ROMディスクに記録すべき暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該CD-ROMディスク内に記録しておき、再生時にはCD-ROMディスク内に記録されている暗号化情報とキー情報を読み出し、CD-ROMディスクから読み出されたキー情報を使用して該暗号化情報を復号化することを特徴とするCD-ROMの記録・再生方式。

【請求項3】 所要の情報が暗号化されて記録されているCD-ROMディスクにおいて、記録された暗号化情報を復号するのに必要なキー情報が該CD-ROMディスク内に記録されていることを特徴とするCD-ROMディスク。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、暗号化された各種情報をCD-ROMディスクに記録し、再生するための、CD-ROMの記録方式、CD-ROMの記録・再生方式、及びCD-ROMディスクに関するものである。

【0002】

【従来の技術】大量の情報を記録するため、レーザ光等を用いた光学式の記録・再生方式が公知であり、このための光ディスクとして、特にコンパクトディスク読出し専用メモリ、所謂CD-ROMディスクがオーディオの分野のみならず各種の分野で広く用いられている。CD-ROMディスクは一般に再生専用型の記録媒体として用いられてきたが、近年追記型のものも開発され、実用に供されている。

【0003】ところで、再生専用型であれ追記型であれ、CD-ROMディスクに書き込まれる情報の機密保持のため、記録すべき情報を暗号化し、この暗号化された情報をCD-ROMディスクに記録するという要求がしばしば生じる。このような要求を満たす1つの技術として、例えば、特開昭64-91256号公報の第4頁上左欄において説明されているように、CD-ROMディスクにユーザデータを記録させる際に暗号データを附加したスクランブル処理を施して暗号化データにして記録させ、CD-ROMドライバにより暗号化データをデ・スクランブル処理を施した後、インターフェースにより復号データ（暗号データと同一）と暗号化データとを

排他論理処理を施してからコンピュータに出力し、これによりユーザデータのセキュリティを確実に行うことができるようとした技術が公知である。この従来技術は、所要の情報をハードウェアを用いて復号化処理する構成であるから、ソフトウェアにより処理を利用する場合に比べ処理の時間を大幅に短縮することができる点に大きな特徴を有している。

【0004】

【発明が解決しようとする課題】しかしながら、上述した従来技術によると、復号化のためのキーとハードウェアとが密接に関連しているため、もしキーの変更が必要な場合にはハードウェアの変更若しくは復号RAM内容の変更をしなければならず、キーの変更のために相当のコストが必要となる。したがって、固定キーを使用し続ける傾向を生じ、第三者がCD-ROMディスクの記録内容を解読するための手掛りを得ることを比較的容易ならしめる結果になるという問題点を有している。これは、CD-ROMディスクに記録すべきデータのフォーマットがISO9660で規格化されているため、同一のキーを継続して使用すると、規格で定められた特定の内容が格納されているアドレスのデータ内容を手掛りに復号化のためのキーを比較的容易に推測することができるとの理由による。そして、このようにして復号化のためのキーが第三者に一旦知れてしまうと、残りのCD-ROMディスクの記録内容も直ちに解読されてしまうという不具合を生じる。

【0005】上記従来技術による他の問題点は、復号化のためのキーの内容は、予め適宜の手段、例えばコードブックに記載しておく等の手段により管理しておかねばならないため、キーの管理が別途必要となり、キー情報管理のためのコストが発生することである。この問題点は上記従来技術のみならず、CD-ROMディスクに暗号化データを記録しようとする場合、一般に生じる問題点である。

【0006】本発明の目的は、したがって、従来技術における上述の問題点、不具合等のうちの1つ又はいくつか、或いは全部を改善することができる、CD-ROMの記録方式、CD-ROMの記録・再生方式、及びCD-ROMディスクを提供することにある。

【0007】本発明の目的をより具体的に例示的に列挙すれば次の通りである。

【0008】CD-ROMディスクに記録すべき情報の暗号化のためのキーの変更に伴うキー情報の管理を不要にした、CD-ROMの記録方式及びCD-ROMの記録・再生方式を提供すること。

【0009】記録された暗号化データの解読のためのキー情報の管理を不要にしたCD-ROMディスクを提供すること。

【0010】暗号化して記録されたデータ内容の解読のためのキーを第三者が容易に知ることができないよう、

コストを上昇させることなしに複数の異なったキーを使用できるようにした、CD-ROMの記録方式及びCD-ROMの記録・再生方式を提供すること。

【0011】CD-ROMディスクに記録すべき情報の暗号化及び暗号化された情報を復号化するために必要なキーを記録媒体毎に容易に変更することができ、且つキーの管理を不要にすることができるようにした、CD-ROMの記録方式、CD-ROMの記録・再生方式及びCD-ROMディスクを提供すること。

【0012】

【課題を解決するための手段】上記課題を解決するため、本発明は、所要の情報を暗号化して光ディスクであるCD-ROMディスクに記録するためのCD-ROMの記録方式において、CD-ROMディスクに記録すべき暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該CD-ROMディスク内に記録しておくことを特徴としている。

【0013】また、本発明は、所要の情報を暗号化してCD-ROMディスクに記録しこの記録された暗号化情報をCD-ROMディスクから読み出して復号化するためのCD-ROMの記録・再生方式において、CD-ROMディスクに記録すべき暗号化情報を復号化するのに必要なキー情報を該暗号化情報と共に該CD-ROMディスク内に記録しておき、再生時にはCD-ROMディスク内に記録されている暗号化情報とキー情報を読み出し、CD-ROMディスクから読み出されたキー情報を使用して該暗号化情報を復号化することを特徴としている。

【0014】さらに、本発明は、所要の情報が暗号化されて記録されているCD-ROMディスクにおいて、記録された暗号化情報を復号するのに必要なキー情報が該CD-ROMディスク内に記録されていることを特徴としている。

【0015】

【作用】所要の情報を暗号化してCD-ROMディスク内に記録する際に、その後このCD-ROMディスクから読み出された暗号化情報を復号化するために必要なキー情報もそのCD-ROMディスク内に記録される。これにより、暗号化情報とこの解読に必要なキー情報を常に一体に管理することができる。

【0016】このような記録方式で暗号化情報が記録されているCD-ROMディスクの記録内容を再生する場合には、暗号化情報と共に所要のキー情報が同一のCD-ROMディスクから読み出され、これらの読み出し情報のみによって暗号化情報を復号化することができ、復号化のためのキー情報を特に意識することなしに所要の復号化が実行される。

【0017】このように、キー情報を適宜に変更しても、CD-ROMディスク内には、記録されている暗号化情報の復号化、すなわち解読に必要なキー情報が必ず

記録されており、キー情報のみの管理は不要である。

【0018】

【実施例】以下、図面を参照して本発明の一実施例につき詳細に説明する。

【0019】図1及び図2には、本発明によりCD-ROMディスクに所要の情報を記録するためのCD-ROM記録システム、及びこれと対をなしてCD-ROM記録・再生システムを構成するCD-ROM再生システムがそれぞれ示されている。

10 【0020】先ず、図1を参照してCD-ROM記録システム10について説明すると、11はCD-ROMディスク1に記録すべきユーザデータが予め格納されている記憶装置、12は各種指令データを入力するためのキーボード、13はキーボード12により指示された所要のユーザデータを記憶装置11から後述するようにして順次読み出すための読み出制御部であり、読み出制御部13によって読み出された所要のユーザデータは暗号化ユニット14に送られる。

【0021】暗号化ユニット14についての説明に先立って、CD-ROMディスク1に所望のユーザデータを記録するための記録方式について図3を参照して説明する。

【0022】図3に示されるように、CD-ROMディスク1の記録領域は、プリギャップ領域2とISO9660領域4とに大別され、ISO9660領域には多数のセクタS1、S2、S3…が設定されている。そして、これらのセクタS1、S2、S3…は、1988年に発行されたISO9660情報交換用CD-ROMのボリューム及びファイルの構造に関するJISX0606-1990に基づくデータフォーマットに従って構成されている。

【0023】したがって、記録すべきデータは、各セクタに設けられている2048バイトのユーザデータ領域に分割して順次格納され、CD-ROMディスク1に記録すべき1セクタ分のデータの内容及びその作成方法についてはその規格に詳述されているので、ここではその詳細を説明するのは省略し、単に、所要のユーザデータは2048バイト分づつISO9660領域4のセクタに分割されて記録されるという点のみを説明するに止める。また、ISO9660領域4では、データフォーマットの定義により未使用領域を定めることができ、本実施例の暗号キー記録セクタ3として使用する。

【0024】図1に戻ると、キーボード12は、さらに、所要のユーザデータをCD-ROMディスク1へ記録するためにそのユーザデータをセクタに分割記録する場合、どのセクタに記録されるユーザデータを暗号化すべきかを示す暗号化セクタ情報を入力する機能を有している。この暗号化セクタ情報はキーボード12から暗号化ユニット14内の暗号キー生成部15へ送られる。

【0025】暗号キー生成部15は、キーボード12か

ら送られてきた暗号化セクタ情報に基づき、ユーザデータを暗号化して記録すべきセクタに対する固有の暗号キーを所要のセクタ毎に生成し、暗号キー情報とその暗号キーが使用されるセクタの番号情報とが組になった複数組の暗号キーデータを作成、保持しておく機能を有している。

【0026】これらの暗号キーデータは、暗号キー記録セクタ3を記録するタイミングでCD-ROMマスタリング装置18に送り、CD-ROMマスタリング装置18によってこれらの暗号キーデータがCD-ROMディスク1内の暗号キー記録セクタ3に記録される(図3参照)。

【0027】一方、読出制御部13は、記憶装置11内に格納されている所要のユーザデータを1セクタ分づつ読み出して暗号化ユニット14の暗号化部16に送る。暗号化部16は、市販の暗号化ICを用いて構成することができ、読出制御部13から1セクタ分のユーザデータを受け取ると、暗号キー生成部15に対し、このセクタに対する暗号キーを暗号化部16へ送るよう要求する暗号キー要求信号を出力する。暗号キー生成部15はこの暗号キー要求信号に応答し、そのセクタに対して暗号キーが用意されている場合には、すなわちそのセクタへ記録すべきユーザデータが暗号化されるべきであるとキー ボード12から指令されている場合には、そのセクタのために予め用意されている暗号キーを暗号化部16に送る。若しそのセクタが暗号化を指令されていないものであり、したがって暗号キーが用意されていない場合には、暗号キー生成部15から暗号化部16へのデータの送信は行わない。

【0028】したがって、暗号化部16では、読出制御部13から1セクタ分づつ送られてくるユーザデータに対し、暗号化が指令されているセクタのものについてだけ暗号キー生成部15から供給される暗号キーを用いて暗号化し、暗号化された1セクタ分のユーザデータをインターフェイス部17に送る。一方、暗号化が指令されていないセクタへ記録すべきユーザデータは暗号化されることなく、そのままインターフェイス制御部17に送られる。

【0029】インターフェイス制御部17では、このようにして暗号化された又は暗号化されていないセクタ毎のユーザデータをCD-ROMマスタリング装置18に順次送り、これらのセクタ毎のユーザデータはCD-ROMディスク1のISO9660領域4に設けられたセクタS1、S2、…に所定の手順によって順次記録される。本実施例では、図3から判るように、セクタS1、S2、S7、S9…に記録されているユーザデータは暗号化されておらず、セクタS3、S6、S8…に記録されているユーザデータは暗号化されている。また、セクタS4、S5は未使用領域として定義し、暗号キーを記録するセクタとして使用される。しか

し、どのセクタのユーザデータを暗号化するか及びどの未使用領域に暗号キーを記録するかは、この一実施例のものに限定されず、適宜に設定することができる。また、キーボード12からその都度指令するのに代えて、暗号化して記録すべきセクタは第1番目から第200番目までなどのように固定化しておいてもよい。

【0030】いずれにせよ、ユーザデータがCD-ROMディスク1内の所定の領域に暗号化されて、又は暗号化されることなしにセクタ情報として記録され、一方、10このようにして記録されたユーザデータを復号化するのに必要な暗号キーがそれと同一のCD-ROMディスク1内の所定の領域に記録されている点に大きな特徴を有している。この特徴による利点の1つは、暗号キーの管理が不要になることであり、特にCD-ROMディスク1に記録された暗号化データを再生して復号化する場合に、外部から別途暗号キー情報を与える必要がないことである。

【0031】なお、上記実施例では、暗号キーをセクタ毎に別のものとしたが、全ての暗号化セクタの暗号キー20を同一にしてもよいことは勿論である。暗号キーを多数用いても暗号キー管理の煩らしさは生じないので、セクタ毎に暗号キーを変えれば、暗号キー管理のコストを上昇させることなしに第三者によるユーザデータの解読を困難にし、機密保持能力を格段に向上させることができる。

【0032】次に、図2を参照して、図1のCD-ROM記録システム10によりCD-ROMディスク1に暗号化して記録されたユーザデータを再生、復号化するためのCD-ROM再生システム20について説明する。

【0033】CD-ROM再生システム20は、CD-ROMディスク1の記録内容を読み取るためのCD-ROMドライブ装置21を有している。CD-ROMディスク1をCD-ROMドライブ装置21にセットすることにより、CD-ROMディスク1の暗号キー記録セクタ3に記録されている暗号キーデータが先ず読み出され、インターフェイス制御部22に送られる。そして、読み出された暗号キーデータは復号化ユニット23内のメモリ25内に格納される。

【0034】かかる後、インターフェイス制御部22の40制御の下に、CD-ROMディスク1内のISO9660領域4に記録されている最初の1セクタ(S1)がCD-ROMドライブ装置21によって読み出され、インターフェイス制御部22を介して復号化部24に送られる。復号化部24もまた、市販の復号化ICを使用して構成することができる。復号化部24では、このセクタS1に対応する暗号キーの読み出しをメモリ25に対して要求する。

【0035】本実施例では、セクタS1は暗号化セクタではないため、メモリ25内にはセクタS1に対応する暗号キーは格納されていない。したがって、メモリ25

からは何等の暗号キー情報は出力されず、セクタS1内に記録されているユーザデータはそのまま復号化部24から出力され、バッファメモリ26内に格納される。セクタS2に記録されているユーザデータも全く同様にして処理される。

【0036】セクタS3の記録内容が復号化部24に入力されると、セクタS3に記録されている暗号化ユーザデータを復号化するのに必要な暗号キーが暗号キーデータ中の番号情報を手掛りとして選択され、所要の暗号キーがメモリ25から復号化部24に送られる。復号化部24では、この暗号キーを用いてセクタS3に記録されていた暗号化ユーザデータの復号化処理が実行され、復号化されたユーザデータがバッファメモリ26に送られる。

【0037】このようにして、セクタS1、S2・・・に記録されていたユーザデータのうち暗号化されていたものは、メモリ25から供給される暗号キーによつて復号されてバッファメモリ26に送られることになる。一方、暗号化されていなかったユーザデータは復号化ユニット23をそのまま通過し、バッファメモリ26に格納される。したがって、バッファメモリ26から、暗号化をする前の所要のユーザデータ、すなわち復号化されたユーザデータを取り出すことができる。また、セクタS4、S5には暗号キーが記録されているが、データフォーマット上未使用領域であり、ユーザデータの取り出しには影響しない。

【0038】図1、図2に示したシステムを用いることにより、少なくとも次の如き効果が期待される。

【0039】ユーザデータを暗号化するのに使用された暗号キーが暗号化されたユーザデータを記録するCD-ROMディスク1内に一緒に記録されるので、暗号化のキー情報を別途管理する必要がない。したがって、暗号キーの管理のためのコストが不要であるばかりか、その管理の煩わしさから解放される。

【0040】さらに、暗号化ユーザデータと暗号キーとを同一CD-ROMディスク1内に記録するので、暗号キーをどのように変更したとしてもこの変更を別途に記録しておく必要はなく、再生時には復号化に必要な暗号キーをそのCD-ROMディスク1から読み出すだけよいから、復号化に要する手間が著しく簡素化される。

【0041】この方式によりユーザデータの暗号化記録が行われたCD-ROMディスク1は、暗号キー情報が記録されているので、CD-ROMディスク1に対応する暗号キー情報の管理という概念ではなく、暗号キー情報管理は全く不要になり、暗号化を全く意識することなしにユーザデータの再生、復号化を行うことができる。

【0042】このように、暗号キー情報の管理コストが全く問題とならないので、例えばCD-ROMディスク1毎に異なる暗号キーを使用しても何等のコストを発生させることができなく、記録の機密保持をコストを生じさ

せることなしに著しく向上させることができる。このことは1枚のCD-ROMディスク1について、各セクタ毎に暗号キーを変更してしまう本実施例の構成についても当然該当するものであり、低コストで第三者の解読が極めて難しい暗号記録が可能である。

【0043】次に図4乃至図6を参照して、コンピュータシステムにおいて所定の記録制御プログラム及び再生制御プログラムを実行させることにより、CD-ROMディスク1の記録、再生を前述の実施例の場合と同様にして行うようにした他の実施例について説明する。

【0044】図4は、CD-ROMディスク1に、外部記憶装置31内に格納されているユーザデータを暗号化して記録すると共に、暗号化して記録されているユーザデータをCD-ROMディスク1から読み出して再生するための、コンピュータシステムを利用した本発明によるCD-ROM記録・再生システム30の概略構成図である。

【0045】図4で、CD-ROMマスタリング装置18及びCD-ROMドライブ装置21は図1及び図2に示されている各装置と同一のものであり、これらの装置18、21及び外部記憶装置31はコンピュータシステム32に接続されている。符号38で示されるのはキーボードである。

【0046】このコンピュータシステム32は、中央演算処理装置(CPU)33、ランダムアクセスメモリ(RAM)34、読み出し専用メモリ(ROM)35及び入出力インターフェイス装置(I/F)36がバス37によって相互に接続されて成る公知の構成である。そして、ROM35内に格納されている記録制御プログラム及び再生制御プログラムがCPU33において実行されることにより、図1及び図2に示した構成の場合と同様にして、CD-ROMディスク1への暗号化ユーザデータの記録、及びこのようにして記録された暗号化ユーザデータの再生、復号化が実行される。

【0047】先ず、図5を参照しながら、CD-ROM記録・再生システム30による記録動作について説明する。

【0048】記録制御プログラムの実行が開始されると、先ずステップ41でキーボード38から入力される暗号化対象セクタを示すデータに従つて暗号化対象セクタが決定される。次のステップ42では、暗号化が必要な各セクタの暗号キーが生成され、生成された暗号キーが暗号キーデータとしてRAM34内に格納される。この暗号キーデータは図1に基づいて説明したものと同様である。

【0049】ステップ43では、CD-ROMマスタリング装置18が暗号キー記録セクタ3への書き込み状態になっているか否かが判別される。CD-ROMマスタリング装置18が暗号キー記録セクタ3への書き込み状態になっていると、ステップ43の判別結果はYESと

なり、ステップ44に進む。ステップ44では、RAM34に格納されている暗号キーデータがCPU33及びI/F36を経由してCD-ROMマスタリング装置18に送られ、CD-ROMマスタリング装置18にセットされているCD-ROMディスク1の暗号キー記録セクタ3に暗号キーデータが記録される。しかる後、ステップ49で所要のユーザデータが全て記録されたか否かの終了チェックが行われ、全ての記録がまだ終了していない場合にはステップ43に戻る。

【0050】暗号キーデータの記録が終了した時点ではステップ43の判別結果はNOとなり、ステップ45において1セクタ分のユーザデータが外部記憶装置31から読み込まれる。次のステップ46では、この読み込まれた1セクタ分のユーザデータを記録すべきセクタが暗号化対象セクタになっているか否かが判別される。その1セクタ分のユーザデータを記録すべきセクタが暗号化対象セクタであると、ステップ46の判別結果はYESとなり、ステップ47に入る。

【0051】ステップ47では、ステップ42で生成された暗号キーのうちそのセクタのための暗号キーを用いて1セクタ分のユーザデータを暗号化するための処理を行い、次のステップ48で暗号化処理された1セクタ分のユーザデータをCD-ROMマスタリング装置18に送る。CD-ROMマスタリング装置18は受け取った1セクタ分のユーザデータを所要のセクタに記録する。

【0052】ステップ46の判別結果がNOの場合にはステップ47は実行されないので、外部記憶装置31から読み込まれた1セクタ分のユーザデータは暗号化処理されず、そのままCD-ROMマスタリング装置18に送られ、所要のセクタに記録される。

【0053】このようにして、ユーザデータが全てCD-ROMディスク1に書き込まれると、ステップ49の判別結果がYESとなり、記録制御プログラムの実行が終了する。

【0054】次に、このようにしてCD-ROMディスク1に記録されたデータをCD-ROMディスク1から読み出し再生するためのCD-ROM記録・再生システム30の再生、復号化動作について、図6を参照しながら説明する。

【0055】再生制御プログラムの実行開始後、先ずステップ51においてCD-ROMディスク1の入替ありか否かが判別される。入替ありの場合にはステップ52に進み、ここで、暗号キー記録セクタ3に記録されている暗号キーデータが読み込まれステップ53に進む。ステップ51の判別結果がNOの場合には、既に暗号キーデータの読み込みはなされているので、ステップ52は実行されず、ステップ53に入る。

【0056】ステップ53では、CD-ROMドライブ装置21によってCD-ROMディスク1から1セクタ分のデータを読み込み、ステップ54でこの読み込まれ

た1セクタ分のデータが復号化対象セクタのデータであるか否かが判別される。それが復号化対象セクタであるとステップ55に入り、ステップ52で既に読み込まれている暗号キーデータのうちのそのセクタに対応する暗号キーデータを用いて所要の復号化処理が行われ、ステップ56に進む。一方、ステップ53で読み込まれた1セクタ分のデータが復号化対象セクタのデータでない場合には、ステップ55を実行することなしにステップ56に入る。

10 【0057】ステップ56では、全ての必要セクタの読み込みが終了したか否かが判別され、全ての必要セクタの読み込みが未だ終了していない場合にはステップ53に戻る。このようにして、CD-ROMディスク1に記録されたデータが1セクタ毎に読み込まれ、復号化の必要なセクタについてのみ復号化処理が実行される。全ての必要セクタの読み込みが終了すると、ステップ56での判別結果がYESとなり、再生制御プログラムの実行が終了する。このようにして、CD-ROMディスク1に記録されたユーザデータを再生、復号化することができる。

【0058】図4に示したCD-ROM記録・再生システム30もまた、図1及び図2に示したシステムの場合と同様の利点を有している。

【0059】

【発明の効果】本発明による効果は以下の通りである。

【0060】CD-ROMディスクに記録すべきデータを暗号化するのに使用された暗号キー情報が暗号化されたデータを記録するCD-ROMディスク内に記録されるので、暗号キー情報を別途管理する必要がない。したがって、暗号キー情報の管理のためのコストが不要であるばかりか、その管理の煩わしさから解放される。

【0061】暗号化データと暗号キー情報を同一のCD-ROMディスク中に記録するので、暗号キーをどのように変更したとしてもこの変更に関する情報を別途に記録、管理しておく必要はなく、CD-ROMディスク内のデータの再生時には復号化に必要な暗号キーをそのCD-ROMディスクから読み出すだけよいから、復号化に要する手間が著しく簡素化される。

【0062】本発明の方式によりデータの暗号化記録が40行われることによって、暗号化データとこれを解読するための暗号キー情報とが一緒に記録されているCD-ROMディスクは、CD-ROMディスクに対応する暗号キー情報の管理という概念ではなく、暗号キー情報管理は全て不要になり、その管理コストを不要にすることができますほか、暗号化を全く意識することなしにユーザデータの再生、復号化を行うことができる。

【0063】暗号キー情報の管理コストが全く問題とならないので、例えばCD-ROMディスク毎に異なった暗号キーを使用しても何らの管理コストを発生させることがなく、記録の機密保持をコストを生じさせることな

しに著しく向上させることができる。

【図面の簡単な説明】

【図1】本発明によるCD-ROMディスクの記録システムの一実施例を示す構成図。

【図2】本発明によるCD-ROMディスク再生システムの一実施例を示す構成図。

【図3】図1及び図2のシステムにおいて使用されるCD-ROMディスクの記錰方式を説明するためのCD-ROMディスク内の記録領域の説明図。

【図4】本発明によるCD-ROMディスク記録・再生システムの他の実施例を示す構成図。

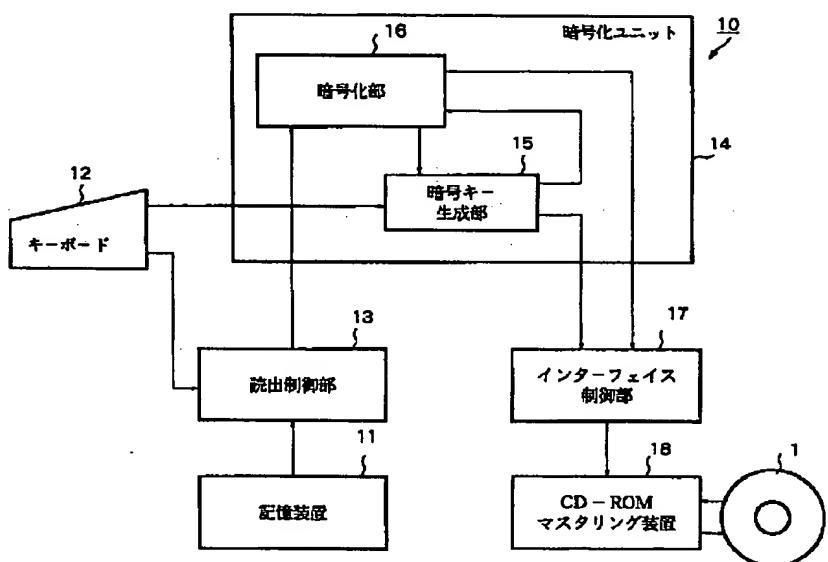
【図5】図4のコンピュータシステムにおいて実行される記録制御プログラムを示すフローチャート。

【図6】図4のコンピュータシステムにおいて実行される再生制御プログラムを示すフローチャート。

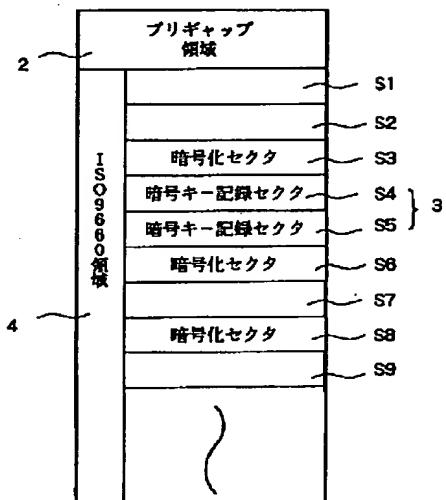
【符号の説明】

- 1 CD-ROMディスク
- 3 暗号キー記録セクタ
- 4 ISO9660領域
- 10 CD-ROM記録システム
- 11 記憶装置
- 14 暗号化ユニット
- 15 暗号キー生成部
- 16 暗号化部
- 17 インターフェイス制御部
- 20 CD-ROM再生システム
- 23 復号化ユニット
- 24 復号化部
- 30 CD-ROM記録・再生システム
- S1乃至S9 セクタ

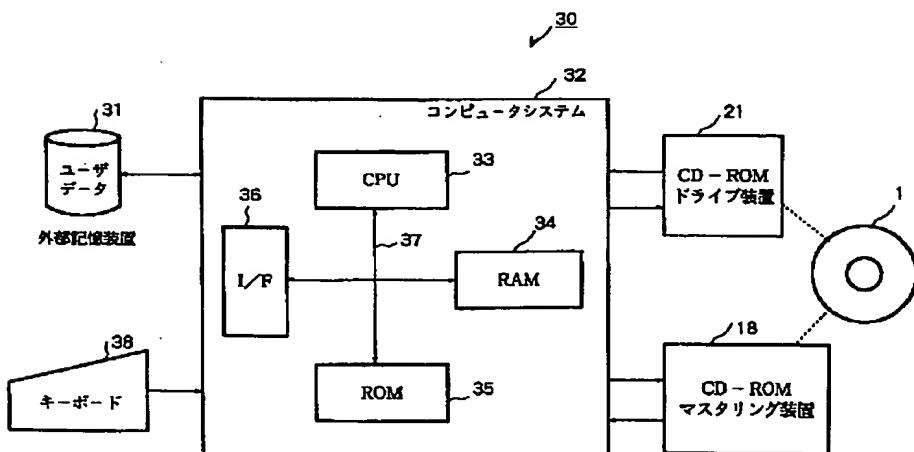
【図1】



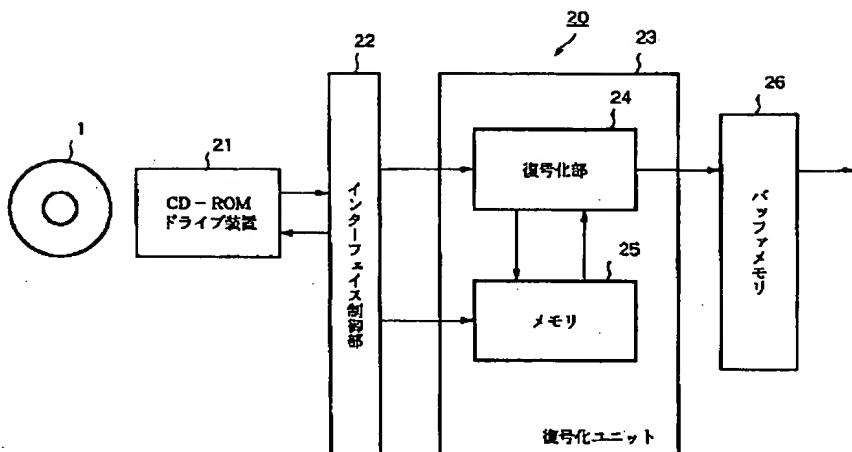
【図3】



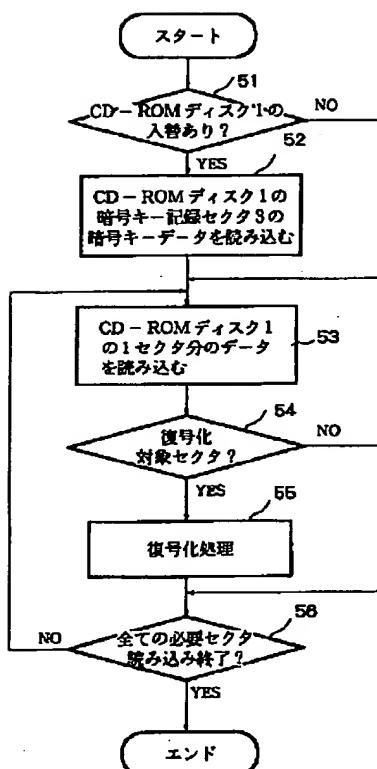
【図4】



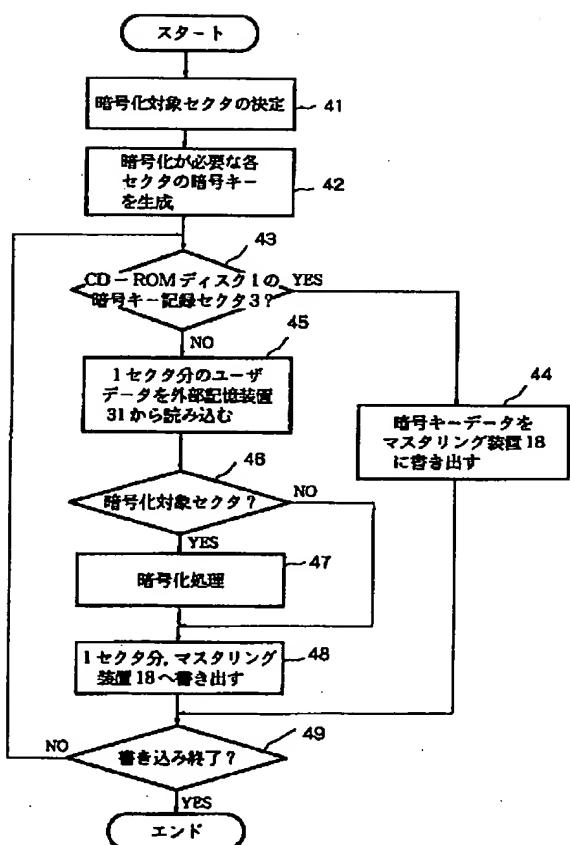
【図2】



【図6】



【図5】



フロントページの続き

(72)発明者 谷口 利典

愛知県名古屋市瑞穂区苗代町15番1号 ブ

ラザーエンジニアリング株式会社内